REMARKS

Applicant would like to thank the Examiner for the thorough examination of the present application. Claims 9, 28, 31 and 34 have been amended to address noted minor informalities. For Claim 31, the amendment is being made so that the claim is consistent with Claims 5, 13 and 21. The arguments supporting patentability of the claims are provided below.

I. The Claimed Invention

The present invention, as recited in independent Claim 1, for example, is directed to a method for securing circulation of an encrypted digital document to be reproduced with a document reader. The method comprises providing a user with a storage device storing identification information identifying the storage device and for storing an identification information list comprising identification information identifying recent document readers previously operated with the storage device.

The method further comprises transmitting to a server over a digital data transmission network from the storage device to the server upon connection of the storage device to the server by a terminal connected to the digital data transmission network and to the storage device information identifying the digital document to be reproduced, and the information list and the identification information of the storage device.

The method further comprises identifying from the server the storage device on the basis of the information identification of the storage device transmitted to the server.

Possible fraudulent use of the storage device is determined based upon the information list that is transmitted to the server. The server compares the identification information in the information list with an authorized or fraudulent reader list for determining fraudulent use of the storage device. If the storage device is not being fraudulently used, then the method comprises transmitting over the digital data transmission network from the server to the computer terminal a decryption key specific to the digital document to be reproduced, with the decryption key being stored in the storage device. The digital document is decrypted using the stored decryption key by the document reader connected to the storage device. The digital document decrypted by the document reader is reproduced.

Independent Claim 9 is also directed to a method for securing circulation of an encrypted digital document to be reproduced with a document reader, and is similar to independent Claim 1.

Independent Claim 17 is directed to a system for securing circulation of an encrypted digital document to be reproduced with a document reader, and is similar to independent Claim 1.

Independent Claim 25 is also directed to a system for securing circulation of an encrypted digital document to be reproduced with a document reader, and is similar to independent Claim 1.

II. The Claims Are Patentable Over Chatani Et Al.

The Examiner rejected independent Claims 1, 9, 17 and 25 over the Chatani et al. published patent application. The Chatani et al. application is directed to a computer network system for securely distributing computer software products. FIG. 1 in Chatani et al. illustrates a block diagram of the computer network system. The Examiner maintains his position that Chatani et al. discloses the claimed invention.

The Applicant submits that the Examiner has mischaracterized Chatani et al. More particularly, Chatani et al. is directed to a product distribution and payment system for limited use or otherwise restricted digital software products. Digital content data comprising a software product to be rented is made available to customers through a detachable local storage medium, such as a DVD or CD-ROM disc, or over a network connection.

The product digital content is capable of being accessed and played back through a computer or game console at the customer's site. The software product may comprise a limited use product that is restricted in the number of plays or duration of use. The customer is allowed to download and purchase the product using his computer or playback console. The product purchase information is encoded and transmitted to the content distributor. When the preset time or number of plays has elapsed the software program is frozen and access to the program is not allowed.

The Applicant submits that Chatani et al. discloses a completely different approach for determining possible fraudulent use of the storage device as compared to the claimed invention. Fraudulent use of the storage device in Chatani et al. is based on the software product being a limited use product. When the software product is purchased, the buyer selects the desired type of limited use product. Reference is directed to paragraph 45 in Chatani et al., which provides:

> " . . . In step **322**, the user follows the instructions of the server to select the purchase option he or she prefers. For a limited use product, the user may be prompted to select between renting the product for a certain period of time or for a certain number of accesses (game plays), or combinations thereof. . . ." (Emphasis added).

The Applicant submits that Chatani et al. fails to disclose that a possible fraudulent use of the storage device is determined based upon an information list that is transmitted to the server, as in the claimed invention. In the claimed invention, the information list comprises identification information identifying recent document readers previously operated with the storage device, and the server compares the identification information in the information list with an authorized reader list for determining fraudulent use of the storage device.

In Chatani et al., the Examiner references paragraph 60 which discloses that when the user makes a purchase, a database record is maintained which records both the serial number of the playback machine and the serial number of the disk. If the user is ever forced to replace their playback machine, he or she could request a new unlock key by inserting the disk into the new playback machine. The database then confirms that the disk serial number shows a purchase against it, and therefore allows a new unlock key to be generated for the user.

The Applicant submits that by keeping track of the disk serial number which shows a purchase against it, there is no need to compare the identification information (i.e., recent document readers previously operated with the storage device) in the information list with an authorized reader list for determining fraudulent use of the storage device. Instead of focusing on an authorized or unauthorized reader list in Chatani et al., Chatani et al. focuses on when the preset time or number of plays has elapsed for the purchased software program. Once one or both of these parameters has elapsed, then the software program is frozen and access to the program is not allowed. The database in Chantani et al. simply confirms that a purchase has been made with respect to the disk via its disk serial number.

In sharp contrast, possible fraudulent use of the storage device in the claimed invention is based upon the information list that is transmitted to the server, and the server compares the identification information in the information list with an authorized reader list for determining fraudulent

use of the storage device. In Chatani et al., replacing the playback machine with a new playback machine has nothing to do with an authorized or unauthorized reader list of recent document readers previously operated.

Chatani et al. merely teaches the use of a database recording, for each disk purchased, the serial number of a single playback machine and the serial number of the purchased disk and the generation of the decryption key on the basis of the serial numbers. This is done in order to control the use of different playback machines for reading a same purchased disk. Chatani et al. fails to disclose a playback machine in which a memory card is determined as fraudulent or unauthorized for further use with any playback machine.

Accordingly, it is submitted that amended independent Claim 1 is patentable over Chatani et al. Amended independent Claims 9, 17 and 25 are similar to amended independent Claim 1. Therefore, it is submitted that these claims are also patentable over Chatani et al. In view of the patentability of amended independent Claims 1, 9, 17 and 25, it is submitted that the dependent claims, which include yet further distinguishing features of the invention are also patentable. These dependent claims need no further discussion herein.

III. CONCLUSION

In view of the arguments provided herein, it is submitted that all the claims are patentable. Accordingly, a Notice of Allowance is requested in due course. Should any minor

informalities need to be addressed, the Examiner is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,

MICHAEL W. TAYLOR
Reg. No. 43,182
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330